

CLAIM AMENDMENTS

This listing of claims will replace all prior versions, and listings, of claims in the application.

- 1 1. (currently amended) A method of file access control comprising:
 - 2 [[a.]] storing an encrypted filename of a file at a location in a computing
 - 3 system;
 - 4 [[b.]] converting the encrypted filename into a plaintext filename;
 - 5 [[c.]] modifying the plaintext filename into a modified filename; and
 - 6 [[d.]] authorizing an entity to access the file for performing a writetype of
 - 7 operation on the file by comparing based on the modified filename to
 - 8 the stored encrypted filename.
- 1 2. (currently amended) The method according to claim 1, wherein said
- 2 converting comprises using a key that comprises a combination of two
- 3 encryption keys to convert the encrypted filename into the plaintext
- 4 filename.
- 1 3. (original) The method according to claim 2, wherein said modifying
- 2 comprises using a first one of the two encryption keys to encrypt the
- 3 plaintext filename into the modified filename.
- 1 4. (original) The method according to claim 3, wherein said authorizing
- 2 comprises using the second one of the two encryption keys to encrypt the
- 3 modified filename to form a result and determining whether the result
- 4 matches the encrypted filename.
- 1 5. (original) The method according to claim 2, wherein said modifying
- 2 comprises using a first one of the two encryption keys to encrypt the
- 3 plaintext filename and performing a hash function on the filename thereby
- 4 forming the modified filename.

- 1 6. (original) The method according to claim 5, wherein said authorizing
- 2 comprises comparing the modified filename to a stored hash value.

- 1 7. (original) The method according to claim 1, wherein said encrypted
- 2 filename is encrypted using a first key prior to said storing and further
- 3 comprising storing a second encrypted filename of the file at the location
- 4 wherein the second encrypted filename is encrypted using a second key
- 5 prior to said storing.

- 1 8. (original) The method according to claim 7, wherein said converting
- 2 comprises using the first key to convert the encrypted filename into the
- 3 plaintext filename.

- 1 9. (original) The method according to claim 8, wherein said modifying
- 2 comprises using the second key to encrypt the plaintext filename into the
- 3 modified filename.

- 1 10. (original) The method according to claim 9, wherein said authorizing
- 2 comprises comparing the modified filename to the second encrypted
- 3 filename.

- 1 11. (original) The method according to claim 10, wherein said modifying
- 2 further comprises performing a hash function on the filename after using
- 3 the second key to encrypt the plaintext filename.

- 1 12. (currently amended) The method according to claim 1, wherein the
- 2 plaintext filename permits read access to the file ~~and wherein said type of~~
- 3 ~~operation is a write operation.~~

- 1 13. (original) The method according to claim 1, wherein said storing
- 2 comprises substituting said encrypted filename into a directory structure at
- 3 the location in place of the plaintext filename.

1 14. (original) The method according to claim 1, further comprising encrypting
2 data of the file.

1 15. (currently amended) An apparatus for controlling access to a file,
2 comprising:

3 [[a.]] a server for the storing an encrypted filename associated with a
4 file; and

5 [[b.]] a client in communication with the server for retrieving the
6 encrypted filename from the server, for converting the encrypted
7 filename into a plaintext filename and for modifying the plaintext
8 filename into a modified filename,

9 wherein the client provides the modified filename to the server and
10 wherein the server determines whether the client is authorized to perform a
11 writetype of operation on the file by comparing based on the modified
12 filename received from the client to the stored encrypted filename.

1 16. (currently amended) The apparatus according to claim 15, wherein the
2 plaintext filename permits read access to the file ~~and wherein the type of~~
3 ~~operation to the file is a write operation~~.

1 17. (currently amended) The apparatus according to claim 15, wherein said
2 client converts the encrypted filename into the plaintext filename using a
3 key that comprises a combination of two encryption keys.

1 18. (original) The apparatus according to claim 17, wherein said client forms
2 the modified filename using a first one of the two encryption keys to
3 encrypt the plaintext filename.

1 19. (currently amended) The apparatus according to claim 18, wherein said
2 server determines whether the client is authorized to perform the write
3 type of operation on the file by using the second one of the two encryption
4 keys to encrypt the modified filename to form a result and determines
5 whether the result matches the encrypted filename provided by the client.

1 20. (currently amended) The apparatus according to claim 17, wherein said
2 client forms the modified filename using a first one of the two encryption
3 keys to encrypt the plaintext filename and performs a hash function on the
4 filename thereby forming the modified filename.

1 21. (currently amended) The apparatus according to claim [[20]]17, wherein
2 said server performs a hash function on the filename to form a result and
3 determines whether the client is authorized to perform the readtype of
4 operation on the file by comparing the result to a stored hash value.

1 22. (original) The apparatus according to claim 17, wherein said client forms
2 the modified filename using a first one of the two encryption keys to
3 encrypt the plaintext filename and performs a hash function on the
4 filename to form a result and wherein the server determines whether the
5 client is authorized to perform the type of operation on the file by
6 comparing the result to a stored hash value.

1 23. (original) The apparatus according to claim 15, wherein the encrypted
2 filename is encrypted using a first key and wherein the server stores a
3 second encrypted filename wherein the second encrypted filename is
4 encrypted using a second key.

1 24. (original) The apparatus according to claim 23, wherein the client
2 converts the encrypted filename into the plaintext filename using the first
3 key and modifies the plaintext filename into the modified filename using
4 the second key.

1 25. (currently amended) The apparatus according to claim 24, wherein the
2 server determines whether the client is authorized to perform the write
3 a type of operation on the file by comparing the modified filename to the
4 second encrypted filename.

1 26. (original) The apparatus according to claim 25, wherein the server
2 performs a hash function on the filename after the client uses the second
3 key to modify the filename.

1 27. (original) The apparatus according to claim 25, wherein the client
2 performs a hash function on the filename after using the second key to
3 modify the filename.

1 28. (currently amended) An apparatus for controlling access to a file
2 comprising a server having a stored encrypted filename of a file, the server
3 being in communication with a writer and a reader, the writer being a
4 client of the server and having a first key that permits the writer to write to
5 the file and the reader being another client of the server and having a
6 combination key that comprises a combination of the first key and a
7 second key wherein the combination key permits the reader to read the
8 file.

1 29. (currently amended) The apparatus according to claim 28, wherein the
2 stored encrypted filename is obtained by encrypting a filename of the file
3 using the combination key of the first key and the second key.

1 30. (original) The apparatus according to claim 29, wherein the server
2 determines that the writer is authorized to write to the file by receiving
3 from the writer the filename encrypted using the first key, encrypting the
4 received filename again using the second key thereby forming a twice
5 encrypted filename and comparing the twice encrypted filename to the
6 stored encrypted filename.

1 31. (original) The apparatus according to claim 29, wherein the server
2 determines that the writer is authorized to write to the file by receiving
3 from the writer the filename encrypted using the first key, applying a hash
4 function to the received filename thereby forming a computed hash value
5 and comparing the computed hash value to a stored hash value.

1 32. (currently amended) An apparatus for controlling access to a file
2 comprising a server having a first stored encrypted filename of the file and
3 a second stored encrypted filename of the file, the server being in
4 communication with a writer and a reader, the writer being a client of the
5 server and having a first key that permits the writer to write to the file and
6 the server determining whether the writer is authorized to write to the file
7 by receiving from the writer the filename encrypted using the second key
8 and comparing the received filename to the second stored encrypted
9 filename and the reader being another client of the server and having a
10 second key that permits the reader to read the file.

1 33. (original) The apparatus according to claim 32, wherein the reader
2 decrypts the first stored encrypted filename using the first key.

1 34. (cancelled)

1 35. (currently amended) The apparatus according to claim [[33]]32, wherein
2 the server performs a hash function on the received filename before
3 comparing the received filename to the second stored encrypted filename.

1 36. (new) The method according to claim 2, further comprising:
2 encrypting the plaintext filename using a key that comprises a
3 combination of two encryption keys; and
4 comparing a result of this encrypting to the stored encrypted filename
5 to determine whether to permit read access to the file.

1 37. (new) The method according to claim 36, wherein said modifying
2 comprises using a first one of the two encryption keys to encrypt the
3 plaintext filename into the modified filename

1 38. (new) The apparatus according to claim 15, wherein the client encrypts
2 the plaintext filename and the server compares the encrypted plaintext
3 filename to its stored encrypted filename to determine whether to permit
4 read access to the file.

1 39. (new) The apparatus according to claim 38, wherein the client encrypts
2 the plaintext filename to form the encrypted plaintext filename using a key
3 that comprises a combination of two encryption keys and the client
4 encrypts the plaintext filename to form the modified filename using a first
5 one of the two encryption keys.